REMARKS

Favorable consideration of this Application as presently amended, and in light of the following discussion is respectfully requested.

Claims 1-5, 11-29, 38-44, and 50 are pending in the application; Claims 1, 11, 21, 22, 38, 39, and 50 are amended, and Claims 6-10, 30-37, and 45-49 are canceled by the present amendment. Support for amended Claims 1, 11, 21, 22, 38, 39, and 50 can be found in the original specification, claims and drawings.[1] No new matter is presented.

In the outstanding Official Action, Claims 39 and 45 were rejected under 35 U.S.C. § 112, second paragraph, as indefinite; Claims 1, 6, 11, 16-22, 25-27, 30, 33-35, 38, 42 and 47 were rejected under 35 U.S.C. § 103 as unpatentable over Zhang et al. (U.S. Patent No. 6,550,008, hereinafter "Zhang"); Claims 2-5, 7-10, 12-15, 28-29, 36-37, 39-41, 43-46 and 48-50 were rejected under 35 U.S.C. § 103 as unpatentable over Zhang in view of Sims III (U.S. Pub. No. 2002/0016919, hereinafter "Sims"); and Claims 23-24 and 31-31 were rejected under 35 U.S.C. § 103 as unpatentable over Zhang in view of Yagawa et al. (U.S. Patent No. 6,751,598, hereinafter "Yagawa").

The Official Action rejected Claims 39 and 45 under 35 U.S.C. § 112, second paragraph, as indefinite. Specifically, the phrase "the key data of the same generation" in Claim 39 is cited as failing to have proper antecedent basis. In response, Claim 39 is amended to simply recite "key data..." instead of "the key ..." Claim 45 is canceled by the present amendment.

Accordingly, Applicants respectfully request that the rejection of Claims 39 and 45 under 35 U.S.C. § 112, second paragraph, be withdrawn.

The Official Action rejected Claims 1, 6, 11, 16-22, 25-27, 30, 33-35, 38, 42 and 47 under 35 U.S.C. § 103 as unpatentable over Zhang. Applicants respectfully assert that

[1] E.g. specification, p. 9.

amended independent Claims 1, 11, 21, 22 and 38 state novel features clearly not taught or rendered obvious by the applied reference.

Amended Claim 1 relates to a contents purveying system including a data processor (e.g. personal computer, etc.) having a reproduction program for reproducing contents data (e.g. music, video, etc.), and a portable reproducing device (i.e. portable MP3 player, etc.) configured to store contents data furnished from the data processor. The system also includes a contents server configured to distribute the contents data over a network to the data processor.

A first master key and a first authentication key are furnished to the reproduction program after the program is installed in the data processor, and contents stored in a compact disc connected to the data processor are acquired using the first master key for storage. The reproduction program then executes authentication with the portable reproducing device using the first master and authentication keys before contents from the compact disc are exchanged between the data processor and the portable reproducing device.

Amended Claim 1 further recites that when the reproduction program receives contents distributed from the contents server to the data processor, a second master key and a second authentication key are provided to the reproduction program. Content data is then acquired from the contents server using the second master key for storage, and authentication is performed between the portable reproducing device using the second authentication and master keys before contents from the server are exchanged between the data processor and the portable reproducing device

The system of Claim 1 allows for increased security relating to content data downloaded from the content server by utilizing a set of keys, different from those used for the handling of data from a conventional compact disc, when handling data furnished from the content server.

Independent Claims 6, 11, 21, 22, 30 and 38 recite substantially similar subject matter as recited in amended Claim 1, but are directed to alternative embodiments.

Turning to the applied reference, Zhang describes a method for protecting information transmitted between a POD module (26) and a host device (24), which are both included in a receiver (20) for receiving content data broadcast from a head end system (14).[2] The receiver transmits "authorization fields" corresponding to each of the POD module and host device to the head end system, which then accesses a database to validate that the receiver components are authorized to receive transmitted content data.[3] Once the POD module and host device are validated, "binding messages" are transmitted to the POD module. Using the binding information, the POD module confirms that the host device is authenticated, sends the binding information to the host device, and generates and stores a shared session key used to exchange data with the host device.[4] Similarly, after the host device receives the binding information, which is used to authenticate the POD module, it generates and stores a session key used to decrypt information received from the POD module.[5] Then, using the shared session key, the POD module is able to cipher contents, received from the head-end system, and transmit this information to the host device which uses the same shared key to decrypt the data.[6]

However, Zhang's system operates in a fundamentally different manner than the system recited in amended Claim 1, and therefore, Zhang fails to teach or suggest specific features recited in amended Claim 1.

Amended Claim 1 recites, *inter alia*, a contents purveying system including a data processor, wherein

---

[2] Zhang, Fig. 1.
[3] Id., col. 5, line 31-col. 6, line 24, and Fig. 3.
[4] Id., col. 6, lines 25-34.
[5] Id., col. 6, lines 35-46.
[6] Id., col. 12, lines 55-67.

> ...a first master key and a first authentication key are furnished to said reproduction program after installing said reproduction program, the contents data stored in ***a compact disc*** connected to the data processor are acquired using said first master key for storage, said reproduction program is configured to execute authentication with said portable reproducing device using the so-furnished first authentication key and first master key before said contents is transmitted/received between said data processor and said portable reproducing device...

While Zhang may assert that the POD module and host device are interchangeable, as discussed in the Advisory Action of August 31, 2005, Zhang's description is clear regarding the role each of these components satisfies in his system. Accordingly, for the remarks that follow, the POD module is discussed in relation to the "data processor" recited in amended Claim 1, and the host device will be discussed in relation to the "portable reproducing device", as recited in amended Claim 1. Any interpretation to the contrary is an unreasonable interpretation of the Claims and Zhang's system, and it would not be possible for Zhang's system to properly function without the POD module and host device performing their roles, as specified in Zhang's specification. While Applicants acknowledge that the hardware and software components of the POD module and host device may be interchangeable, their assigned function for the proper function of Zhang's system is clear.

Zhang describes that the POD module is configured to receive encrypted contents from a data server, decrypt the contents, and encrypt the decrypted contents (using the above-described shared session key) to be transmitted to the host device in the receiver.[7] Zhang specifically describes that the encryption key used by the POD module to receive contents from the head-end system is ***not*** the same key used to exchange data with the host device, but is instead a session key generated based on the binding messages from the head-end unit, as discussed above.[8] Further, as noted in the Advisory Action, the POD module and/or host

[7] Id.
[8] Id., Figs. 5-6, col. 11, line 19-col. 14, line 36.

device may include various forms of memory configured to store information such as authorization fields, binding messages, transmitted content from the head-end system, software instructions etc. However, none of this information is described as being accessed, and/or exchanged with another device by any type of key or cryptographic method. Therefore, Zhang fails to teach or suggest a first master key for storage which is used to acquire content data from a compact disc whatsoever.

As noted above, amended Claim 1 recites, "a first master key and a first authentication key are furnished to said reproduction program after installing said reproduction program (in the data processor), the contents data stored in ***a compact disc*** connected to the data processor are acquired using said first master key for storage". Zhang fails to teach or suggest such a feature. Instead, as discussed above, Zhang describes that data transmitted from the head-end unit to the POD module is exchanged using a secret key associated with the receiver, but fails to teach or suggest that content data stored in a ***compact disc*** connected to the POD module is retrieved using any key, whatsoever. Zhang describes that the POD module may include a memory in the form of a compact disc, but also describes that the data contained therein is not accessed by a key, nor is there any rationale for such memory to be accessed using a master key for storage.

Amended Claim 1 also recites that the "reproduction program is configured to execute authentication with said portable reproducing device using the so-furnished first authentication key and first master key before said contents is transmitted/received between said data processor and said portable reproducing device". Thus, the same key master key used to obtain the content from the compact disc is used (along with the first authentication key) to authenticate the portable reproducing device with the data processors. Zhang, however, fails to teach or suggest that a first master key is used to retrieve contents data from

a compact disc at the POD device whatsoever, much less that a first set of keys is used to authenticate the host device before transmitting such content data to the host device.

However, even if data from a compact disc were to be exchanged between the POD module and host device, the same master key would not be used for such authentication and acquisition from the compact disc. As noted above, Zhang describes that the authentication procedure, and the generation of session keys, between the POD module and the host device takes place based on an authentication procedure with the head-end unit. Based on the authentication procedure between the POD module, host device and head-end unit, a session key is generated for the exchange of information between these two devices, and this session key and the associated authentication has nothing to do with a master key used to acquire any data from a compact disc.

Amended Claim 1 further recites, *inter alia*, a contents purveying system including a data processor , wherein

> ...when contents data is distributed from said contents server to said reproduction program a second master key different from said first master key and a second authentication key different from the first authentication key are furnished over the network, the contents data furnished from said contents server are acquired using the so-furnished second master key for storage, and authentication with respect to the portable reproducing device is performed using the so-furnished second authentication key and the second master key before said contents is transmitted/received between said data processor and said portable reproducing device....

Thus, the contents data is acquired by the processor using a second master key for storage, and before transmitting the content from the data processor to the portable reproducing device, authentication is performed using the same second master key for storage (along with a second authentication key) between the data processor and the portable reproducing device.

Zhang, however, fails to teach or suggest receiving second authentication and master keys over a network at the POD module, and using the second master key to both obtain data

over the network and perform authentication with the host device. As discussed above, Zhang describes that the POD module and host device generate a session key to exchange content data based on the binding messages received from the head-end unit. However, this session key is not the same as the "conditional access protocol" encryption used to receive and decrypt the information received at the POD module from the head-end unit.[9] Thus, while Zhang describes that information is retrieved from the head-end unit that allows the POD module and host device to perform mutual authentication and generate a session key, this session key used to exchange contents is not the same as the key used by the POD module to retrieve and decrypt content received from the head-end unit. Therefore, Zhang fails to teach or suggest using a second master key for storage for both acquiring data from a contents server and performing authentication between the data processor and the portable reproduction device.

Accordingly, for at least the reasons discussed above, Applicants respectfully request that the rejection of Claims 1 under 35 U.S.C. § 103 as unpatentable over Zhang be withdrawn. For substantially the same reasons as given with respect to amended Claim 1, it is also submitted that amended independent Claims 6, 11, 21, 22, 30 and 38 also patentably define over Zhang.

Claims 2-5, 7-10, 12-15, 28-29, 36-37, 39-41, 43-46 and 48-50 were rejected under 35 U.S.C. § 103 as unpatentable over Zhang in view of Sims. As discussed above, Zhang fails to teach or suggest specific features recited in the pending independent Claims. Likewise Sims fails to remedy this deficiency, and therefore, none of the cited references, neither alone nor in combination, can be asserted as disclosing Applicants Claims 2-5, 12-15, 28-29, 39-41, 43-44 and 50, which include the above distinguished limitation by virtue of independent

[9] Id., col. 10, lines 18-29.

recitation or dependency. Therefore the Official Action does not provide a *prima facie* case of obviousness with regard to any of these claims.

Accordingly, Applicant respectfully requests that the rejection of Claims 2-5, 12-15, 28-29, 39-41, 43-44 and 50 under 35 U.S.C. § 103 as unpatentable over Zhang in view of Sims be withdrawn.

The Official Action has rejected Claims 23, 24, 31 and 32 under 35 U.S.C. § 103 as being unpatentable over Zhang in view of Yagawa et al. (U.S. Patent No. 6,751,598, hereinafter Yagawa).

As discussed above, Zhang fails to teach or suggest specific above-noted features recited in the pending independent Claims. Likewise Yagawa fails to remedy this deficiency, and therefore, none of the cited references, either alone or in combination, can be asserted as disclosing Applicants Claims 23 and 24, which include the above distinguished limitation by virtue of dependency. Therefore the Official Action does not provide a *prima facie* case of obviousness with regard to any of these claims.

Accordingly, Applicant respectfully requests that the rejection of Claims 23 and 24 under 35 U.S.C. § 103 as unpatentable over Zhang in view of Yagawa be withdrawn.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-5, 11-29, 38-44, and 50 is definite and patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959

I:\ATTY\ATH\PROSECUTION\20'S\209462-US\209462 RCE-AM 10.8.05.DOC